BusyBox a Dnsmasq

Petr Krčmář, Ondřej Caletka

7. března 2015

BusyBox: unixový švýcarský nůž

ROOT.CZ CESNET

Co je to BusyBox?

- spousta unixových utilit v jedné binárce
- ± 600 KB (v Debianu)
- 206 příkazů = 3 KB na příkaz
- `busybox --list |wc -l`
- lze zkompilovat různě
- hodí se do embedded zařízení
- pro Linux, OpenWRT, Android

Jak se spouští?

- bez parametrů vypíše seznam příkazů
- jako parametry je možné uvést příkaz
- možné doplnit `--help` pro nápovědu k příkazu
- možno vytvořit symlinky

```
mkdir bbdir
for i in $(busybox --list)
  do
    ln -s busybox bbdir/$i
 done
```

Co všechno obsahuje?

- práce se soubory: cp, mv, rm, dd, ln…
- práce s adresáři: mkdir, rmdir, find…
- komprese: ar, bzip2, gzip, tar, lzma…
- síť: ip, ifconfig, ping, nc…
- skriptování: awk, grep, cut, sort…
- systém: ps, df, du, free, passwd…
- další: mount, modprobe, depmod, md5, sha…
- a další: ash, rpm, cal…
- a ještě další…

Špeky, které se hodí

- co asi nevíte a překvapí vás
- pozor na to, že jde o odlehčené varianty
- obvykle chybí funkcionalita nebo je zjednodušená
- přesto je příjemné tento švýcarský nůž vlastnit

wget

- jednoduché stažení z HTTP nebo FTP
- umí navazovat (-c)
- umí měnit výstupní adresář a soubor
- umí měnit User-Agent
- neumí ukazovat rychlost
- jen ETA a velikost absolutní i relativní

ipcalc

- velmi zjednodušená verze
- umí ukazovat broadcast, síť, masku a prefix
- neumí ukazovat rozsahy

Příklad

```
$ busybox ipcalc -bnmp 192.168.1.10/26
NETMASK=255.255.255.192
BROADCAST=192.168.1.63
NETWORK=192.168.1.0
PREFIX=26
```

vi

- velmi jednoduchý editor
- perfektně použitelný pro editaci konfigurace
- možnosti lze vypsat pomocí `vi -H`
- vyhledávání
- opakování příkazu
- kopírování/vložení
- nastavení pomocí :set
- prostě Vi!

httpd

- jednoduchý web server
- užitečné pro předání souborů po LAN
- neumí directory listing
- ale umí index.html
- umí změnit port, uživatele, adresář
- umí spouštět CGI skripty
- umí jednoduchou autentizaci uživatelů

udhcpd

- DHCP server
- existuje i klient udhcpc
- parametrem je konfigurační soubor
- umí zapisovat do syslogu
- příklad konfigurace...

Příklad konfigurace

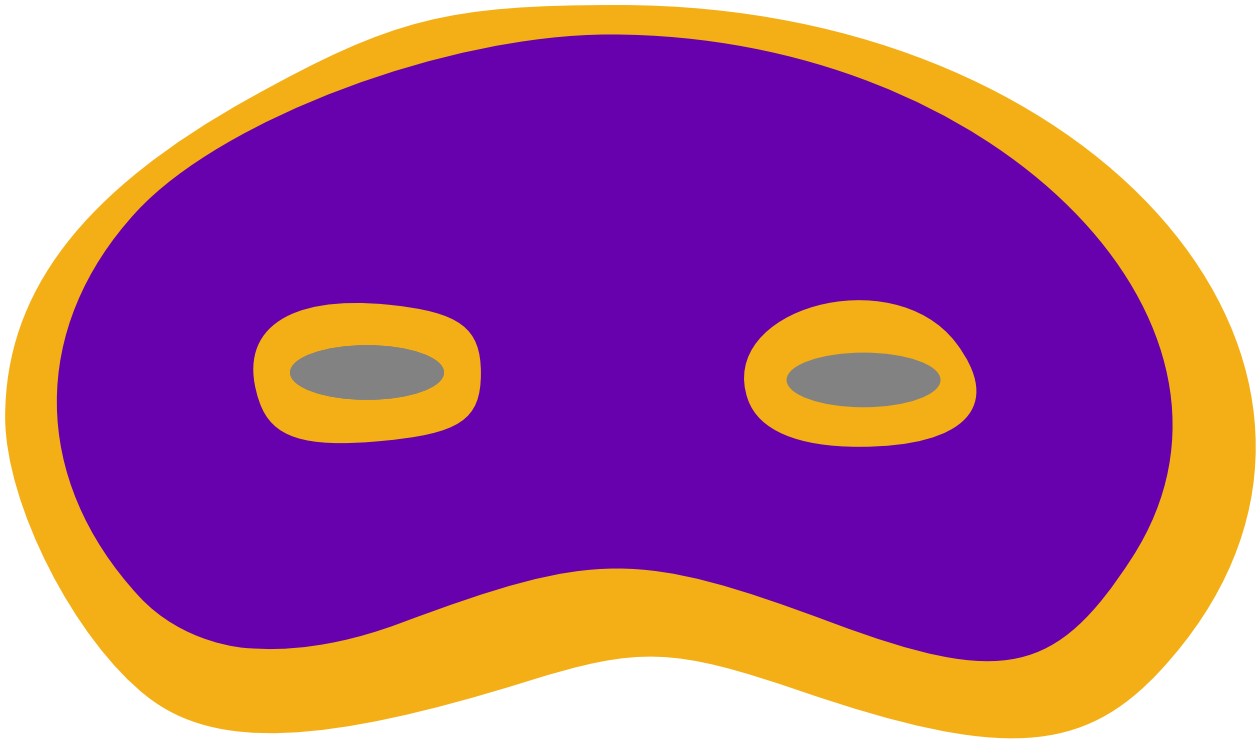
/etc/udhcpd.conf

```
# The start and end of the IP lease block
start 192.168.0.20
end 192.168.0.254

# The interface that udhcpd will use
interface eth0

# Opts
opt dns 192.168.10.2 192.168.10.10
option subnet 255.255.255.0
opt router 192.168.10.2
opt wins 192.168.10.10
option dns 129.219.13.81
option domain local
option lease 864000
option msstaticroutes 10.0.0.0/8 10.127.0.1
option staticroutes 10.0.0.0/8 10.127.0.1, 10.11.12.0/24 10.11.12.1
```

Interní příkazy

```
[, [[, acpid, addgroup, adduser, adjtimex, ar, arp, arping, ash, awk, basename, beep,
blkid, brctl, bunzip2, bzcat, bzip2, cal, cat, catv, chat, chattr, chgrp, chmod, chown,
chpasswd, chpst, chroot, chrt, chvt, cksum, clear, cmp, comm, cp, cpio, crond, crontab,
cryptpw, cut, date, dc, dd, deallocvt, delgroup, deluser, depmod, devmem, df, dhcprelay,
diff, dirname, dmesg, dnsd, dnsdomainname, dos2unix, dpkg, du, dumpkmap, dumpleases, echo,
ed, egrep, eject, env, envdir, envuidgid, expand, expr, fakeidentd, false, fbset, fbsplash,
fdflush, fdformat, fdisk, fgrep, find, findfs, flash_lock, flash_unlock, fold, free,
freeramdisk, fsck, fsck.minix, fsync, ftpd, ftpget, ftpput, fuser, getopt, getty, grep,
gunzip, gzip, hd, hdparm, head, hexdump, hostid, hostname, httpd, hush, hwclock, id,
ifconfig, ifdown, ifenslave, ifplugd, ifup, inetd, init, inotifyd, insmod, install,
ionice, ip, ipaddr, ipcalc, ipcrm, ipcs, iplink, iproute, iprule, iptunnel, kbd_mode,
kill, killall, killall5, klogd, last, length, less, linux32, linux64, linuxrc, ln, loadfont,
loadkmap, logger, login, logname, logread, losetup, lpd, lpq, lpr, ls, lsattr, lsmod,
lzmacat, lzop, lzopcat, makemime, man, md5sum, mdev, mesg, microcom, mkdir, mkdosfs,
mkfifo, mkfs.minix, mkfs.vfat, mknod, mkpasswd, mkswap, mktemp, modprobe, more, mount,
mountpoint, mt, mv, nameif, nc, netstat, nice, nmeter, nohup, nslookup, od, openvt,
passwd, patch, pgrep, pidof, ping, ping6, pipe_progress, pivot_root, pkill, popmaildir,
printenv, printf, ps, pscan, pwd, raidautorun, rdate, rdev, readlink, readprofile, realpath,
reformime, renice, reset, resize, rm, rmdir, rmmod, route, rpm, rpm2cpio, rtcwake,
run-parts, runlevel, runsv, runsvdir, rx, script, scriptreplay, sed, sendmail, seq,
setarch, setconsole, setfont, setkeycodes, setlogcons, setsid, setuidgid, sh, sha1sum,
sha256sum, sha512sum, showkey, slattach, sleep, softlimit, sort, split, start-stop-daemon,
stat, strings, stty, su, sulogin, sum, sv, svlogd, swapoff, swapon, switch_root, sync,
sysctl, syslogd, tac, tail, tar, taskset, tcpsvd, tee, telnet, telnetd, test, tftp, tftpd,
time, timeout, top, touch, tr, traceroute, true, tty, ttysize, udhcpc, udhcpd, udpsvd,
umount, uname, uncompress, unexpand, uniq, unix2dos, unlzma, unlzop, unzip, uptime, usleep,
uudecode, uuencode, vconfig, vi, vlock, volname, watch, watchdog, wc, wget, which, who,
whoami, xargs, yes, zcat, zcip
```

Dnsmasq: vše pro domácí maškarádu



1. nastavit směrování/NAT v kernelu
2. nainstalovat a spustit Dnsmasq
3. PROFIT!

Dnsmasq

- kompletní user-space řešení pro internetovou bránu
  - DNS forwarder
    - s částečným kešováním
    - s vyvažováním zátěže mezi servery
    - s DNSSEC validací
  - DHCP server
  - DHCPv6 server
  - Generátor IPv6 *Router Advertisments*
  - TFTP/PXE server
- velmi často používaný
  - domácí routery
  - tethering v Androidu
  - cache v Ubuntu

DNS forwarder

- původní a asi nejčastěji využívaná funkce
- nedokáže řešit rekurzivní dotazy, vyžaduje nadřazené rekurzivní servery v `/etc/resolv.conf`
- narozdíl od glibc se vyrovná s výpadkem některého z nadřazených serverů
- kešování některých druhů DNS záznamů
- podpora neveřejných domén
- podpora DNSSEC validace
  - nutno zapnout a nastavit body důvěry
  - nepodporuje aktualizaci bodu důvěry (RFC 5011)
  - v základním nastavení **nekontroluje legitimitu nepodepsaných domén**
  - dokáže se vyrovnat s nenastavenými hodinami

Příklad použití DNS forwarderu

```
# dnsmasq --dnssec --trust-anchor=.,19036,8,2,49…B5 \
> --dnssec-check-unsigned --interface=lo
```

Nebezpečné praktiky

neuvedení rozhraní vznikne otevřený rekurzivní server

volba `filterwin2k` cenzura SRV dotazů – přestane fungovat SIP, XMPP, Kerberos,...

neuvedení `check-unsigned` k obejití DNSSEC validace stačí odstranit podpisy

DHCP server

- jednoduchý, přitom ale plnohodnotný server podporující DHCPv4 i DHCPv6
- podpora poolů, vyhrazených adres, různých skupin
- možnost identifikace IPv6 klientů také podle MAC adresy (jsou-li na stejné L2 síti)
- provázání s DNS, automatická registrace DHCP zápůjček do privátní DNS zóny
- PXE server
  - speciální sada DHCP voleb
  - umožňuje při síťovém bootu zobrazit menu
  - alternativa k přímému bootu konkrétního souboru

TFTP server

- read-only TFTP server
- určen pouze pro podporu PXE bootu
- vždy je nutné nastavit `tftp-root`

Příklad DHCP a TFTP

```
# dnsmasq … --dhcp-range=10.0.0.100,10.0.0.110 \
> --dhcp-authoritative --server=/localnet/ \
> --enable-tftp --tftp-root=/tftproot \
> --dhcp-boot=pxelinux.0
```

Příklad PXE menu

```
# dnsmasq …  --pxe-service=x86PC,"Local boot" \
> --pxe-service=x86PC,"Boot.oskarcz.net",bon \
> --pxe-service=x86PC,"Boot.salstar.sk",salstar
```

Podpora IPv6

- nahradí radvd i DHCPv6 server
- registruje klienty do DNS i pro SLAAC
- dokáže identifikovat klienty MAC adresou

Stavové DHCPv6 s RA

```
# dnsmasq … --enable-ra \
  --dhcp-range=::1,::400,constructor:eth0 \
  --dhcp-host=00:11:22:33:44:55,mujstroj,[::42]
```

SLAAC s bezestavovým DHCPv6

```
# dnsmasq … --enable-ra \
  --dhcp-range=::,constructor:eth0,ra-stateless
```

Dnsmasq - závěr

- provázanost služeb je někdy velkou výhodou
- dnsmasq jako *stub resolver* na lokálním stroji
  - zlepší uživatelský zážitek
  - minimální úsilí ke zprovoznění
  - minimální riziko selhání
- unbound je ale bezpečnější a rychlejší
  - ale není úplně bezpečné zapnout zároveň DNSSEC a předávání nadřazeným serverům
  - použití režimu plné rekurze zase přetěžuje globální DNS infrastrukturu a zdržuje
- černé prvenství dnsmasq
  - nejrozšířenější otevřený rekurzivní server na Internetu
  - navíc v historických verzích

ROOT.CZ CESNET

Závěr

Děkujeme za pozornost

Petr Krčmář
Petr.Krcmar@iinfo.cz
http://www.PetrKrcmar.cz

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz